Deutscher Bundestag **Drucksache 18/9445**

18. Wahlperiode 22.08.2016

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Korte, Frank Tempel, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/9334 –

Pläne der Bundesregierung für eine neue Cybersicherheitsstrategie

Vorbemerkung der Fragesteller

Nach Medienberichten von „ZEIT ONLINE“ und dem Deutschlandfunk vom 7. Juli 2016 plant die Bundesregierung die Verabschiedung einer neuen „Cybersicherheitsstrategie für Deutschland 2016“. Ein Referentenentwurf werde gegenwärtig zwischen den zuständigen Bundesministerien abgestimmt und soll im Herbst 2016 vom Kabinett verabschiedet werden. Entstehen soll demnach eine größere und fast militärische Sicherheitsarchitektur für den digitalen Raum, bestehend aus verschiedenen Behörden, die nicht nur beraten, sondern auch schnell handeln können soll. Der Strategie zufolge sollen gleich drei mobile Eingreiftruppen, sogenannte „Quick Reaction Forces“ zum Zweck der Strafverfolgung und der zivilen Gefahrenabwehr aufgebaut werden. Daneben sollen verschiedene Gremien und Behörden, darunter das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Cyber-Abwehrzentrum (Cyber-AZ) des Bundes in Bonn, stark ausgebaut, Polizei, Bundeswehr, Regierung und Wirtschaft stärker miteinander vernetzt werden. Laut den Medienberichten soll außerdem mit einem nationalen Computer Emergency Response Team (CERT) eine weitere Institution gegründet werden, um sofort auf eventuelle Angriffe reagieren zu können. Ferner prüfe die Bundesregierung, ob Hersteller haftbar gemacht werden können, wenn sie Sicherheitsmängel in ihrer Software und ihrer Hardware nicht beheben (vgl. ZEIT ONLINE vom 7. Juli 2016). Außerdem erklärte der Bundesminister des Innern, Dr. Thomas de Maizière, gegenüber dem ZDF-Morgenmagazin: „Wir wollen dass die Provider selbst eine Haftung und Verantwortung dafür übernehmen, wenn Straftaten in ihrem Netz stattfinden“ (ZDF-Morgenmagazin vom 21. Juli 2016).

Vorbemerkung der Bundesregierung

Mit der derzeit gültigen „Cyber-Sicherheitsstrategie für Deutschland“ wurden bereits im Jahr 2011 wesentliche Festlegungen mit dem Ziel einer Erhöhung der Cyber-Sicherheit in Deutschland getroffen. Auch das im vergangenen Jahr in Kraft getretene IT-Sicherheitsgesetz hat seine Grundlage in der Cyber-Sicherheitsstrategie aus dem Jahr 2011.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 18. August 2016 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Die strategischen Ansätze und Ziele der Cyber-Sicherheitsstrategie 2011 haben im Wesentlichen auch heute noch Bestand. Die sich stetig ändernden Rahmenbedingungen machen es aber erforderlich, sie zu ergänzen und in einer neuen Strategie zu bündeln. Die Bundesregierung plant daher, die Cyber-Sicherheitsstrategie weiter zu entwickeln und fort zuschreiben. Derzeit laufen hierzu die regierungsinternen Abstimmungen. Es existiert noch kein zwischen den beteiligten Bundesressorts abgestimmter Text, auf den bei Beantwortung der hier gegenständlichen Kleinen Anfrage Bezug genommen werden könnte. Die nachfolgenden Fragen sind daher für die Bundesregierung aus faktischen Gründen teilweise nur eingeschränkt beantwortbar.

Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit Anfragen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung aber zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann (BVerfGE 124, Seite 161, 189). Evident geheimhaltungsbedürftige Informationen muss die Bundesregierung nach der Rechtsprechung des Bundesverfassungsgerichts nicht offenlegen (BVerfGE 124, 161, 193 f.).

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Fragen 17a und 29 aus Geheimhaltungsgründen teilweise nicht in dem für die Öffentlichkeit einsehbaren Teil beantwortet werden können.

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Die teilweise Einstufung der Antwort auf die Fragen 17a und 29 als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ ist aber im vorliegenden Fall erforderlich. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Fragen würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis – auch der Bundesrepublik Deutschland möglicherweise gegnerisch gesinnten Kräften – nicht nur im Inland, sondern auch im Ausland zugänglich machen.

Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Entwicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt würden. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Diese Informationen werden daher gemäß § 3 Nummer 4 VSA als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

1. Treffen die Pressemeldungen über Pläne der Bundesregierung für eine neue „Cybersicherheitsstrategie für Deutschland 2016“ zu, und wann soll diese verabschiedet werden bzw. in Kraft treten?

Nach derzeitigem Planungsstand soll die neue Cybersicherheitsstrategie 2016 (CSS) im Herbst dieses Jahres durch das Bundeskabinett beschlossen werden. Im Übrigen wird auf die Ausführungen in der Vorbemerkung der Bundesregierung verwiesen.

2. In welcher Weise soll die Strategie parlamentarisch beraten werden?

Eine parlamentarische Beratung der Cybersicherheitsstrategie 2016 als Strategiepapier der Bundesregierung ist nicht vorgesehen.

3. Welche Pläne existieren für einen Ausbau des BSI?

Die Bundesregierung plant die Kapazitäten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auszubauen (s. Seite 103 des Koalitionsvertrages von CDU, CSU und SPD).

4. Welche Pläne existieren für einen Ausbau des Cyber-AZ des Bundes in Bonn, welche Behörden sollen daran in welchem Umfang beteiligt werden, und wer wird nach diesen Plänen zukünftig die Federführung innehaben?

Das Nationale Cyber-Abwehrzentrum in Bonn wird nach derzeitigen Plänen Gegenstand der CSS werden. Konkrete Angaben können mit Hinweis auf den Stand der Arbeiten zur Entwicklung der CSS nicht gemacht werden (siehe Vorbemerkung der Bundesregierung).

5. Inwieweit wird bei den Plänen der Bundesregierung die grundsätzliche Kritik des Bundesrechnungshofs am Cyber-AZ, wonach dessen Einrichtung nicht gerechtfertigt und sein Nutzen „fraglich“ sei, da die jetzige Konzeption „nicht geeignet [sei], die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyberraum zu bündeln“ (Süddeutsche Zeitung vom 7. Juni 2014), berücksichtigt?

Die Kritik des Bundesrechnungshofs wird bei der Weiterentwicklung des Cyber-AZ (Cyberabwehrzentrum) berücksichtigt.

6. Soll das Cyber-AZ nach Plänen der Bundesregierung wesentlich umstrukturiert werden, um sinnvoller zu arbeiten?

   Wenn ja, in welcher Form soll das im Detail geschehen?

Detaillierte Ausführungen zum Umfang der Umstrukturierung und zur Umstrukturierung selbst können mit Hinweis auf die Vorbemerkung der Bundesregierung nicht gemacht werden.

7. Hat die Bundesregierung selbst eine Evaluation des Cyber-AZ durchführen lassen, und wenn ja, mit welchem Ergebnis?

   Wenn nein, warum nicht?

Das Bundesministerium des Innern begann vor der Prüfung des Bundesrechnungshofs mit einer Evaluierung. Diese Evaluierung hat bereits zu einer Verbesserung der Arbeit im Cyber-AZ geführt und ist als laufender Prozess der Fortentwicklung noch nicht abgeschlossen.

8. Wie weit wurden die Planungen des Bundesministeriums des Inneren (BMI) zur Einrichtung von zwei Unterabteilungen „IT- und Cybersicherheit, sichere Informationstechnik“ und „Cybersicherheit im Bereich der Polizeien und des Verfassungsschutzes“ (heise.de, „Innenministerium: zwei neue Stäbe für die Cybersicherheit“, 13. Juni 2014) umgesetzt, was sind ihre Aufgaben, wie viel Personal wurde dorthin aus welchen anderen Abteilungen versetzt, und wie viel neu gewonnen?

Zur Verbesserung der Aufgabenwahrnehmung im Bereich Cyber wurden im Bundesministerium des Innern (BMI) im Jahr 2014 in den Abteilungen Öffentliche Sicherheit und IT zwei neue Stäbe „IT- und Cybersicherheit; sichere Informationstechnik“ und „Cybersicherheit im Bereich der Polizeien und des Verfassungsschutzes“ eingerichtet, die sich einerseits mit Strafverfolgung und Spionageabwehr, andererseits mit der präventiven, Technik-gestaltenden Seite der Cybersicherheit befassen. Die Einrichtung bedingte einen Aufwuchs von vier Referaten in der Abteilung Informationstechnik, Digitale Gesellschaft und Cybersicherheit (IT) und eines Referates in der Abt. Öffentliche Sicherheit (ÖS) mit entsprechender Personalausstattung. Die Mitarbeiter wurden vorrangig durch Straffung der bisherigen Aufbauorganisation aus den Abteilungen ÖS und IT selbst gewonnen.

9. Ist es nach Einschätzung der Bundesregierung mit Hilfe der Cyber-Abwehrabteilung im BMI besser als mit dem Cyber-AZ gelungen, die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyberraum zu bündeln?

Mit der Einrichtung der Stäbe wurden die fachaufsichtliche Aufgabenwahrnehmung sowie die Zusammenarbeit der Behörden weiter gestärkt. Dies umfasst auch die Zusammenarbeit der Behörden im Cyber-AZ. Eine vergleichende Aussage ist daher nicht möglich.

10. Wie soll die zivil-militärische Zusammenarbeit zwischen Cyber-AZ und Bundeswehr im Detail neu konzipiert werden?

Die Bundeswehr ist seit dem Jahr 2011 im Cyber-AZ vertreten. Dies wird sie auch in Zukunft sein. Im Übrigen bleiben die Aufgaben und Zuständigkeiten der Ressorts unberührt. Des Weiteren wird auf die Vorbemerkung der Bundesregierung verwiesen.

11. Treffen die Medienberichte zur Einrichtung des CERT zu, und wenn ja,

    a) handelt es sich dabei um eine tatsächlich neue Einrichtung oder die seit dem 1. September 2001 beim BSI bestehende „CERT-Bund“;

    b) was soll sich nach den bisherigen Planungen organisatorisch, personell und bei den Zuständigkeiten für das CERT bzw. CERT-Bund ändern;

    c) welche genaue Rolle ist ihm innerhalb der Cybersicherheitsstrategie zugedacht;

    d) mit welchen Kosten für Personal und Technik rechnet die Bundesregierung (bitte entsprechend aufschlüsseln)?

Die Fragen 11 und 11a bis 11d werden gemeinsam beantwortet.

Mit der neuen Cyber-Sicherheitsstrategie der Bundesregierung sollen die CERT-Strukturen (Computer Emergency Response Team) in Deutschland weiter gestärkt werden. Im Übrigen wird auf die Ausführungen in der Vorbemerkung der Bundesregierung verwiesen.

12. Inwieweit sind Cyber-AZ und CERT in den Ausbau der für offensive Cyber-Einsätze trainierenden CNO-Einheit (CNO – Computer Networks Operation) der Bundeswehr eingebunden?

Eine Einbindung des Cyber-AZ bzw. CERT-Bund in den Ausbau der CNO-Einheit der Bundeswehr (Computer Netzwerk Operation) ist nicht vorgesehen.

13. Trifft es zu, dass der BND die „Lagebildaufklärung“ in fremden Netzen übernimmt oder übernehmen soll und seine Ressourcen im Konfliktfall den CNO-Kräften der Bundeswehr zur Verfügung stellt?

Die Beantwortung der Frage 13 kann aus Gründen des Staatswohls nicht in offener Form erfolgen. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik des Bundesnachrichtendienstes und insbesondere seinen Aufklärungsaktivitäten und Analysemethoden stehen. Der Schutz vor allem der technischen Aufklärungsfähigkeiten des Bundesnachrichtendienstes im Bereich der Fernmeldeaufklärung stellt für die Aufgabenerfüllung des Bundesnachrichtendienstes einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität nachrichtendienstlicher Informationsbeschaffung durch den Einsatz spezifischer Fähigkeiten und damit dem Staatswohl. Eine Veröffentlichung von Einzelheiten betreffend solcher Fähigkeiten würde zu einer wesentlichen Schwächung der den Nachrichtendiensten zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies würde für die Auftragserfüllung des Bundesnachrichtendienstes erhebliche Nachteile zur Folge haben. Sie kann für die Interessen der Bundesrepublik Deutschland schädlich sein. Insofern könnte die Offenlegung entsprechender Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „Geheim“ eingestuft.[*]

14. Wie viele öffentliche und nicht öffentliche Einrichtungen betreiben in der Bundesrepublik Deutschland ein CERT (bitte so weit wie möglich nach Verwaltung, Wirtschaft und Universitäten/Forschungseinrichtungen differenzieren), die im Deutschen CERT-Verbund zusammengeschlossen sind?

Im CERT-Verbund gibt es derzeit 41 Mitglieder, die sich wie folgt aufschlüsseln lassen:

- Verwaltung: 9
- Wirtschaft: 30
- Forschung: 2.

[*] Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

15. Existiert mittlerweile der „Verbund Deutscher Verwaltungs-CERT“, was sind seine Aufgaben und Tätigkeitsfelder, und wer hat die Geschäftsführung inne?

Der VerwaltungsCERT-Verbund (VCV) wurde im Jahr 2013 formal gegründet und ist mittlerweile – nach Aufbau der CERTs in den Ländern – operativ tätig. Im VCV findet ein Austausch zu Sicherheitsthemen inklusive Bewertung, technischer Analyse und Abstimmung von Maßnahmen statt. Schwachstelleninformationen werden vertraulich ausgetauscht. Eine zentrale Geschäftsführung ist aufgrund der partnerschaftlichen Kooperation auf gleicher Ebene nicht vorgesehen.

16. Welche externen Beraterinnen und Berater waren und sind bei der Ausarbeitung der „Cybersicherheitsstrategie für Deutschland 2016“ in welcher Form und Funktion tätig, und welche Kosten entstehen dadurch jeweils (bitte entsprechend nach den genannten Kategorien auflisten)?

Die Ausarbeitung des Entwurfstextes der neuen Cybersicherheitsstrategie 2016 erfolgt derzeit durch die beteiligten Bundesressorts unter Federführung des Bundesministeriums des Innern. Externe Beraterinnen und Berater sind hieran nicht beteiligt.

17. Trifft es zu, dass im BMI Pläne existieren, wonach künftig mit dem Bundesamt für Verfassungsschutz (BfV), dem Bundeskriminalamt (BKA) und dem BSI gleich drei Behörden jeweils eine digitale Eingreiftruppe (Quick Reaction Force) aufbauen, die jederzeit ausrücken kann?

    Wenn ja, wie sehen diese Pläne konkret aus?

Ja.

a) Wann soll das „Cyber-Team“ des BfV einsatzbereit sein, aus wie vielen Personen soll es bestehen, mit welchen Ressourcen soll es ausgestattet werden, und welche Aufgaben soll es auf welcher Rechtsgrundlage übernehmen?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.*

b) Wann soll die Quick Reaction Force des BKA einsatzbereit sein, aus wie vielen Personen soll sie bestehen, mit welchen Ressourcen soll sie ausgestattet werden, und welche Aufgaben soll sie auf welcher Rechtsgrundlage übernehmen?

Beim Bundeskriminalamt (BKA) soll noch im Jahr 2016 die Einrichtung einer Quick Reaction Force (QRF) erfolgen. Die QRF ist eine jeweils aus vier Cybercrime-Experten des BKA bestehende, rotierende 24/7-Rufbereitschaft, um notwendige polizeiliche Sofortmaßnahmen außerhalb der Regelarbeitszeit einzuleiten. Rechtsgrundlage für die Einrichtung der QRF ist § 4 Absatz 1 Nummer 5 a) und b) des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG).

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Anlage ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

c) Wann soll das Mobile Incident Response Team (MIRT) des BSI einsatzbereit sein, aus wie vielen Personen soll es bestehen, mit welchen Ressourcen soll es ausgestattet werden, und welche Aufgaben soll es auf welcher Rechtsgrundlage übernehmen?

Die Mobile Incident Response Teams (MIRTs) des BSI sollen im Jahr 2017 ihre Arbeit aufnehmen. Die MIRTs des BSI werden gemäß § 3 Absatz 1 Satz 2 Nummer 2 und § 3 Absatz 3 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) auf Ersuchen und mit Einwilligung von Bundesbehörden, Verfassungsorganen und Betreibern Kritischer Infrastrukturen vor Ort schnell, flexibel und adressatengerecht bei der technischen Bewältigung von Sicherheitsvorfällen unterstützen. Ziel dieser Unterstützung ist die schnellstmögliche Wiederherstellung eines sicheren technischen Betriebs der betroffenen Einrichtung.

d) Sollen die Mitglieder der genannten neuen Einheiten durch Neustrukturierungen und Umsetzungen oder durch Neugewinnung von Personal gewonnen werden, und wie hoch schätzt die Bundesregierung den entstehenden Personalbedarf?

Die Mobile Incident Response Teams des BSI sind Gegenstand des Regierungsentwurfs des Bundeshaushalts 2017ff. Die Ergebnisse der parlamentarischen Beratungen des Haushaltsentwurfs bleiben abzuwarten.

Auch hinsichtlich der QRF des BKA und der Cyber-Teams des Bundesamtes für Verfassungsschutz (BfV) sind noch keine belastbaren Aussagen möglich, da die Konzepte für die Einheiten noch nicht abschließend abgestimmt sind.

18. Wie und auf welcher Rechtsgrundlage soll die jeweilige Zuständigkeit der Quick Reaction Forces geregelt und sollen mögliche Kompetenzprobleme vermieden werden?

Die notwendige Koordination bei Einsätzen verschiedener Behörden erfolgt wie auch sonst im Bereich Cyber-Sicherheit auf Bundesebene unter Wahrung der verfassungsrechtlichen Grenzen und rechtlichen Vorgaben im Nationalen Cyber-Abwehrzentrum.

19. Wie soll verhindert werden, dass das Trennungsgebot zwischen Polizei und Nachrichtendiensten verletzt wird und sich Zuständigkeiten überschneiden?

Auf die Antwort zu Frage 18 wird verwiesen.

20. Trifft es zu, dass im BMI Pläne existieren, wonach das BMI zusammen mit den Providern die „Sensorik im Netz ausbauen“ will, um Cyberangriffe und Infektionen besser erkennen zu können und laufende Angriffe abzuschwächen?

Wenn ja:

a) Was ist konkret mit „Sensorik“ gemeint?

b) Auf welcher jeweiligen Rechtsgrundlage soll dies ggf. erfolgen?

c) Welche entsprechenden Einrichtungen (honey pots etc.) werden dazu bereits von den Netzbetreibern in der Bundesrepublik Deutschland betrieben, und welche Defizite hat die Bundesregierung hierbei erkannt?

d) Fällt darunter auch eine sogenannte „Deep Packet Inspection“?

Nein.

21. Soll künftig der komplette Netzwerkverkehr automatisiert überwacht werden, und wenn ja, von wem soll dies auf welche Weise und auf welcher Rechtsgrundlage erfolgen?

    Wenn nein, in welchem Umfang und auf welche Weise soll dann die Überwachung auf welcher konkreten Rechtsgrundlage erfolgen?

Seitens der Bundesregierung ist keine automatisierte Überwachung des kompletten Netzwerkverkehrs geplant.

22. Existieren in der Bundesregierung oder einzelnen Geschäftsbereichen Planungen mit dem Ziel, den Straftatenkatalog in § 100a der Strafprozessordnung (StPO) zu erweitern, und wenn ja, welche Straftatbestände oder kriminologischen Phänomenbereiche kommen hierfür in Betracht?

Im Rahmen der Expertenkommission StPO (Strafprozessordnung) wurde eine Anpassung des Straftatenkatalogs des § 100a Absatz 2 StPO diskutiert. Eine abschließende Entscheidung innerhalb der Bundesregierung zu einer Umsetzung der Empfehlungen der Expertenkommission wurde noch nicht getroffen.

23. Um welche Straftaten handelt es sich nach Auffassung der Bundesregierung konkret, „die online und konspirativ verübt werden“ und demnach in den Straftatenkatalog des § 100a StPO aufgenommen werden müssten?

Auf die Antwort zu Frage 22 wird verwiesen.

24. Plant die Bundesregierung eine „Anpassung“ der Mitwirkungspflichten von Unternehmen, etwa bei der Identifizierung von Nutzern, und wenn ja, wie soll diese Anpassung im Detail aussehen?

Mit der Einführung einer Verifizierungspflicht für Prepaid-Nutzer im Mobilfunk ist bereits eine entsprechende Anpassung der Mitwirkungspflichten von Unternehmen erfolgt. Darüber hinaus kann mit Hinweis auf die Vorbemerkung der Bundesregierung keine Aussage getroffen werden.

25. Wie können und sollen nach Auffassung der Bundesregierung eine Haftung und Verantwortung der Provider konkret geregelt werden, wenn Straftaten in deren Netzen stattfinden, und wie kann sichergestellt werden, dass Provider ihre Netze auf kriminelle Handlungen und Inhalte hin überprüfen, ohne dass sie dabei ihrerseits eine gesetzwidrige Überwachungsinfrastruktur aufbauen?

26. Kann die Bundesregierung ausschließen, dass darunter Pflichten auch für deutsche Anbieter von anonymen Internetdiensten sein werden?

Die Fragen 25 und 26 werden gemeinsam beantwortet.

Die Bundesregierung plant derzeit keine Initiativen zur Regelung der Haftung und Verantwortung der Zugangs-Provider, wenn Straftaten in deren Netzen stattfinden.

Die Bundesregierung prüft jedoch, inwieweit Mitwirkungspflichten von Host-Providern und Plattformbetreibern angepasst werden können, um die Verbreitung strafbarer Inhalte auf den Plattformen effektiv einzuschränken. In diesem Zusammenhang strebt die Bundesregierung eine Überprüfung des unionsrechtlich verankerten Host-Provider-Privilegs an.

Darüber hinaus ist zu beachten, dass Host-Provider nur unter den Bedingungen der §§ 7 bis 10 des Telemediengesetzes (TMG) strafrechtlich verantwortlich gemacht werden können, die auf Artikel 12 bis 15 der E-Commerce-Richtlinie beruhen.

27. Ist es korrekt, dass Pläne existieren, der Staat müsse sich stärker für private Sicherheitsdienstleister öffnen, weil es nach Auffassung der Bundesregierung in den Sicherheitsbehörden an Fachkräften mangele?

Wenn ja:

a) In welchen Bereichen und für welche Aufgaben will das BMI mehr private Sicherheitsfirmen einsetzen?

c) Wie kann oder soll nach Auffassung der Bundesregierung die Datensicherheit bei der Beauftragung privater Unternehmen z. B. bei der Datenweitergabe etc. gewährleistet werden?

d) Sieht die Bundesregierung insbesondere bei der Beauftragung nichtdeutscher privater Unternehmen Sicherheitsrisiken, und wenn ja, welche sind dies?

Die Fragen 27, 27a, 27c und 27d werden gemeinsam beantwortet.

Aus Sicht der Bundesregierung haben Staat und Wirtschaft in Zeiten des IT-Fachkräftemangels ein gemeinsames Interesse daran, den gegenseitigen Austausch von IT-Fachwissen und die Bildung von Spezialisten-Netzwerken zu befördern. Bei der technischen Bewältigung von IT-Sicherheitsvorfällen und bei sonstigen Maßnahmen zur Erhöhung der IT-Sicherheit durch das BSI müssen im Rahmen des geltenden Rechts auch private vertrauenswürdige IT-Firmen eingebunden werden, wenn dies aus technischen oder ressourcenmäßigen Gründen erforderlich ist. Dies ist zum Beispiel in § 3 Absatz 3 BSIG für die Unterstützung von Betreibern Kritischer Infrastrukturen, in § 7 Absatz 1 Satz 2 BSIG für die Zusammenarbeit mit Providern bei öffentlichen Warnungen oder in § 7a Absatz 1 Satz 2 BSIG für Produktuntersuchungen durch das BSI vorgesehen. Dem Schutz personenbezogener Daten, der staatlichen Geheimhaltung und dem Schutz von Dienstgeheimnissen wird bei der Zusammenarbeit ebenso Rechnung getragen wie dem Schutz von Betriebs- und Geschäftsgeheimnissen von Unternehmen.

b) Inwieweit soll die Bundeswehr künftig bei der Cyberabwehr Unterstützung durch zivile Akteure erhalten?

Die Bundeswehr lässt den Großteil ihrer Informationstechnik im Inland durch die BWI Informationstechnik GmbH (BWI IT) betreiben. Die BWI IT hat ein Computer Emergency Response Team (CERTBWI) eingerichtet, welches das CERT der Bundeswehr bei der Bearbeitung von IT-Sicherheitsvorkommnissen unterstützt. Darüber hinaus wird das CERTBw im Rahmen bestehender Verträge mit der Firma Symantec bei der Bearbeitung von IT-Sicherheitsvorkommnissen und mit der Firma Microsoft bei der Erstellung von Konfigurationsvorgaben unterstützt. Zudem ist die Bundeswehr grundsätzlich an darüber hinausgehenden Unterstützungsleistungen, wie die Unterstützung bei der Erfassung von aktuellen Informationen zur Bedrohungslage, interessiert. Zu Art und Umfang solcher Leistungen bestehen derzeit jedoch keine konkreten Pläne.

28. Ist es zutreffend, dass Pläne bestehen, wonach im BMI außerdem eine zentrale Stelle entstehen soll, die „Cyberwaffen" (Hard- und Software zur Infiltration und zum aktiven Eindringen in fremde Computersysteme) beschafft und entwickelt, und wenn ja, aus welchen Gründen wird dies für nötig erachtet, und auf welcher jeweiligen Rechtsgrundlage soll dies passieren?

Auf die Antwort der Bundesregierung zu Frage 1 der Kleinen Anfrage der Faktion DIE LINKE. auf Bundestagsdrucksache 18/9311 vom 1. August 2016 wird verwiesen.

Die Errichtung der zentralen Stelle soll aufgrund von Artikel 65 Satz 2 des Grundgesetzes per Errichtungserlass erfolgen.

29. Was muss als Aufgabe dieser neuen Stabsstelle im BMI unter der Formulierung „technische Unterstützung für nationale Sicherheitsbehörden im Hinblick auf deren operative Cyberfähigkeiten" im Detail verstanden werden (bitte ausführen)?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.*

30. Ist es zutreffend, dass die Bundesregierung derzeit prüft, ob Hersteller haftbar gemacht werden können, wenn sie Sicherheitsmängel in ihrer Software und ihrer Hardware nicht beheben, und wenn ja,

a) welche Ergebnisse hat diese Prüfung bereits erbracht;

b) plant die Bundesregierung eine entsprechende Überarbeitung des IT-Sicherheitsgesetzes?

Die Fragen 30, 30a und 30b werden gemeinsam beantwortet.

Die Bundesregierung sieht die Hersteller von Hard- und Software in der Pflicht, Sicherheitsmängel in ihren Produkten zeitnah und proaktiv zu beheben. Im Rahmen der Verhandlungen des Richtlinien-Vorschlags für Verträge über digitale Inhalte wird die Frage nach (Sicherheits-Updates im Zusammenhang mit der Mängelgewährleistung im Vertragsverhältnis „Unternehmer-Verbraucher" diskutiert. Darüber hinaus sieht die Bundesregierung derzeit keinen gesetzgeberischen Handlungsbedarf.

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch" eingestuft. Die Anlage ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333